CLAIMS

What is claimed is:

1. A method comprising:

   generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve;

   publishing a public key corresponding to the isogeny;

   encrypting a message using a encryption key corresponding to the isogeny; and

   decrypting the encrypted message using a decryption key corresponding to the isogeny.

2. A method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny.

3. A method as recited by claim 1, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof.

4. A method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

5. A method as recited by claim 1, wherein the decrypting is performed by bilinear pairing.

6. A method as recited by claim 5, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

7. A method as recited by claim 1, wherein the method is applied using Abelian varieties.

8. A method as recited by claim 1, wherein the method signs the message.

9. A method as recited by claim 1, wherein the method provides identity based encryption.

10. A method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves.

11. A method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

12. A method as recited by claim 1, further comprising using a trace map to shorten points on an Abelian variety.

13. A method comprising:

publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; and

decrypting an encrypted message using a decryption key corresponding to the isogeny.

14. A method as recited by claim 13, wherein the decryption key is a dual isogeny of the isogeny.

15. A method as recited by claim 13, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof.

16. A method as recited by claim 13, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

17. A method as recited by claim 13, wherein the decryption is performed by bilinear pairing.

18. A method as recited by claim 17, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

19. A method as recited by claim 13, wherein the method is applied using Abelian varieties.

20. A method as recited by claim 13, wherein the method signs the message.

21. A method as recited by claim 13, wherein the method provides identity based encryption.

22. A method as recited by claim 13, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

23. A system comprising:

a first processor;

a first system memory coupled to the first processor, the first system memory storing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve;

a second processor;

a second system memory coupled to the second processor, the second system memory storing an encrypted message and a decryption key corresponding to the isogeny to decrypt the encrypted message,

wherein the encrypted message is encrypted using an encryption key.

24. A system as recited by claim 23, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny.

25. A system as recited by claim 23, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

26. A system as recited by claim 23, wherein the decryption is performed by bilinear pairing.

27. A system as recited by claim 26, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

28. One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; and

decrypting an encrypted message using a decryption key corresponding to the isogeny.

29. One or more computer-readable media as recited by claim 28, wherein the decryption key is a private key, the private key being a dual isogeny of the isogeny.

30. One or more computer-readable media as recited by claim 28, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof.

31. One or more computer-readable media as recited by claim 28, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

32. One or more computer-readable media as recited by claim 28, wherein the decrypting is performed by bilinear pairing.

33. One or more computer-readable media as recited by claim 32, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

34. One or more computer-readable media as recited by claim 28, wherein the acts are applied using Abelian varieties.

35. One or more computer-readable media as recited by claim 28, wherein the acts further comprise using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

36. One or more computer-readable media as recited by claim 28, wherein the acts further comprise composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves.

37. One or more computer-readable media as recited by claim 28, wherein the acts further comprise using a trace map to shorten points on an Abelian variety.

38. One or more computer-readable media as recited by claim 28, wherein the acts sign the message.

39. One or more computer-readable media as recited by claim 28, wherein the acts provide identity based encryption.